

Application No. 10/574,909
Reply to Office Action of July 25, 2008

Docket No.: 4005-0277PUS1
Page 5 of 9

REMARKS

Applicants appreciate the Examiner's thorough consideration provided the present application. Claims 1-10 are currently pending in the application. Claims 1, 2 and 4 have been amended to better define the present invention. Claims 6-10 have been added to define additional aspects of the invention. Claims 1 and 6 are independent. Reconsideration of this application is respectfully requested.

Interview with the Examiner

Applicants' representative thanks the Examiner for the courtesies extended during the telephonic interview conducted on January 23, 2009.

In the interview with the Examiner, Applicants' representative discussed proposed claim amendments in relation to the rejection of claim 1 under 35 U.S.C. §101. During the interview, the Examiner indicated that if claim 1 were amended so that it was clear the enciphering device was combining the polynomials, the current §101 rejection would be reconsidered. In this Reply, claim 1 has been amended in accordance with the discussions conducted with the Examiner.

Claim Rejection Under 35 U.S.C. §101

Claims 1, 2, 4 and 5 are rejected under 35 U.S.C. § 102(b) as allegedly being directed to non-statutory subject matter. In accordance with the discussion with the Examiner during the aforementioned interview, Applicants have amended claim 1. Accordingly, Applicant respectfully requests that the Examiner withdraw the §101 rejection of claims 1, 2, 4 and 5.

KM/JAV

Application No. 10/574,909
Reply to Office Action of July 25, 2008

Docket No.: 4005-0277PUS1
Page 6 of 9

Claim Rejections Under 35 U.S.C. §103

Claims 1-4 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schwan (U.S. Pat. Appln. Pub. No. 2004/0187035) in view of known techniques (e.g., U.S. Pat. No. 4,922,539 to Rajasekaran). Claim 5 was rejected under 35 U.S.C. 103(a) as being unpatentable over Schwan in view of known techniques, and further in view of Applied Cryptography, Protocols, Algorithms, and Source Code in C, by Bruce Schneier (hereinafter Schneier). Applicants respectfully traverse these rejections.

Independent claim 1 currently recites:

A method of protecting a cryptographic algorithm (6) before introduction in an enciphering device (1) comprising programmable processor unit (4), the algorithm being separable into the form of initial polynomials (P_i) of at least two variables each, and having a degree of not less than two, the method comprising:

providing to the enciphering device at least two initial polynomials (P_i , P_{i+1});

combining, on the enciphering device, combined polynomials (Q_k), each obtained from the at least two initial polynomials (P_i , P_{i+1}); and

implementing the combined polynomials (Q_k) in the programmable processor unit (4).

(Emphasis added.)

Applicants respectfully submit that the above combination of elements as set forth in amended independent claim 1 is not disclosed nor suggested by the references relied on by the Examiner.

As mentioned in prior replies, Schwan does not teach or suggest protecting the algorithm **before** it is introduced in a device but when it is implemented in the device. To this effect

KM/JAV

Application No. 10/574,909
Reply to Office Action of July 25, 2008

Docket No.: 4005-0277PUS1
Page 7 of 9

Schwan combines two features (see [0007] and [0008]): an encapsulation of the algorithm and a control of access to the data input. Those features have nothing in common with the method of separating the algorithm into initial polynomials and combining them for safe transport.

In the Office Action, the Examiner attempts to cure the deficiency of Schwan by asserting the underlined feature quoted above in claim 1 is inherent. Specifically, the Examiner states that "MPEP 2112(I) states that the claiming of a new use, new function, or unknown property which is inherently present in the prior art does not necessarily make the claim patentable." (See Office Action: page 3, para. 8, lines 6-9.)

Applicants submit the feature is not inherent in Schwan, as Schwan merely teaches implementing a control unit for technical installations that utilizes cryptographic algorithm to prevent unauthorized access. The device taught by Schwan allows modification "only if authenticity was previously detected by certain information ... by input of a PIN, or by dynamic variable authentication by a challenge response method." (See [0012].) Accordingly, Schwan teaches protection of a control algorithm after introduction into a device (see [0007]-[0009]), but fails to provide any specific teaching regarding the protecting of a cryptographic algorithm before introduction in an enciphering device, as recited above.

Rajasekaran fails to cure this deficiency of Schwan, as Rajasekaran merely teaches a form of polynomial factorization used in a speech processing context.

Accordingly, neither of the references utilized by the Examiner individually or in combination teaches or suggests the limitations of amended independent claim 1 or its dependent claims 2-4. Therefore, Applicants respectfully submit that claim 1 and its dependent claims clearly define over the teachings of the references relied on by the Examiner.

KM/JAV

Application No. 10/574,909
Reply to Office Action of July 25, 2008

Docket No.: 4005-0277PUS1
Page 8 of 9

Regarding claim 5, Schneier fails to cure the deficiencies of Schwan and Rajasekaran with respect to claim 1. Claim 5 is therefore allowable at least by virtue of its dependency from claim 1.

Accordingly, reconsideration and withdrawal of the rejections under 35 U.S.C. §103 are respectfully requested.

KM/JAV

RECEIVED
CENTRAL FAX CENTER

JAN 26 2009

Application No. 10/574,909
Reply to Office Action of July 25, 2008Docket No.: 4005-0277PUS1
Page 9 of 9**CONCLUSION**

It is believed that a full and complete response has been made to the Office Action, and that as such, the Examiner is respectfully requested to send the application to Issue.

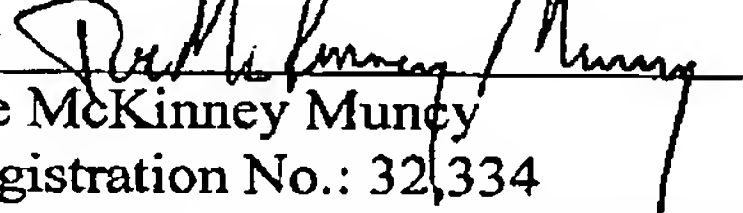
In the event there are any matters remaining in this application, the Examiner is invited to contact Joe McKinney Muncy, Registration No. 32,334 at (703) 621-7140 x101 in the Washington, D.C. area.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicants respectfully petition for a three (3) month extension of time for filing a response in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 50-3828 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Dated: January 26, 2009 (Monday)

Respectfully submitted,

By 
Joe McKinney Muncy
Registration No.: 32,334
MUNCY, GEISLER, OLDS, AND LOWE, PLLC
Centreponte II
Suite 310 East
P.O. Box 1364
Fairfax, Virginia 22038-1364
(703) 621-7140 x101
Attorney for Applicant

KM/JAV